(57) **Abstract**

The invention relates to a method to authenticate a mobile station B in a mobile network, so that the mobile station B is authenticated and an encryption key is agreed between mobile stations A and B using user data exchange during call setup. More specifically the mobile station B is authenticated by the mobile station A constructing and sending to the mobile station B a message M_1, the mobile station B receiving the message M_1, constructing and sending a message M_2 to the mobile station A, the mobile station A receiving the message M_2, checking the validity of the information in the message M_2, if the information is verified valid the mobile station A accepting to share a shared encryption key K with mobile station B, the mobile station A constructing and sending the message M_3 to the mobile station B, the mobile station B receiving the message M_3 and verifying the validity of the information, if the information is valid the mobile station B accepting the sharing of the shared encryption key K with the mobile station A.

Figure 3